Certificados Digitais e PKI (Public Key Infraestructure)

- A infra-estrutura de chave pública (Public-Key Infraestructure – PKI) oferece uma série de vantagens para uma organização
  - Pode ser utilizada a fim de suportar os serviços de segurança: autenticação; integridade; confidencialidade e não-repúdio
  - Facilita a administração da tecnologia pois uma única solução pode atender os vários requisitos de segurança, ao invés do uso de múltiplas soluções
  - Permite a redução do número de senhas solicitadas aos usuários e desta forma minimiza os custos associados ao gerenciamento destas senhas
  - Reduz a necessidade de papéis e permite um fluxo de trabalho que pode ser automatizado com maior segurança e eficiência
  - Permite que a equipe de TI tenha foco no negócio
  - Reduz requisitos de treinamento relativos à segurança, pois devido ao uso de uma única solução para segurança

Criptografia Simétrica

- Os cifradores simétricos possuem características desejáveis como:
  - Pequena implementação
  - Grande velocidade no processo de cifragem/decifragem
- Porém, em certos casos, possuem alguns inconvenientes:
  - Necessidade da troca da chave
  - Dificuldade para iniciar uma comunicação segura
  - Falta de escalabilidade
  - Estes inconvenientes podem ser minimizados com o uso de um KDC (Key Distribuition Center) porém esta técnica também sofre limitação

Criptografia Assimétrica

- A criptografia assimétrica fornece alguns importantes serviços como:
  - Segurança entre partes que não se conhecem
  - Cifragem / Decifragem
  - Assinatura Digital
  - Integridade de Dados
  - Troca de Chaves

Criptografia Assimétrica Serviços

- Segurança entre partes que não se conhecem
  - Isto pode ser feito a partir da disseminação da chave pública, o que não implica em necessariamente em uma falha de segurança considerando a dificuldade para calcular a chave privada a partir da chave pública
  - Para disseminar a chave pública pode ser criado um repositório onde estas chaves seriam armazenadas
  - Para iniciar a comunicação com outro lado (por exemplo Alice com Bob) é necessário:
    - Que Alice confie no repositório ou,
    - Possua uma maneira de confiar na informação. Neste caso o repositório não é confiável, porém existe uma maneira independente de verificar a informação (Isto pode ser feito com um certificado de chave pública)

Criptografia Assimétrica Serviços – Cifragem/Decifragem

- Cifragem / Decifragem
  - Os algoritmos de chave pública podem ser utilizados para cifragem/decifragem, porém o processo é bem mais lento tornando-se normalmente impraticável na maioria das aplicações.
  - Normalmente o processo utilizado utiliza os seguinte passos:
    - Os dados são cifrados utilizando uma chave simétrica (K) gerada de forma randômica
    - A chave simétrica é então cifrada utilizando a chave pública (PU) e enviada ao destinatário
    - Ao receber a chave cifrada o destinatário utiliza sua chave privada (PR) a fim de decrifar a mensagem e obter a chave simétrica (K)
    - A chave simétrica obtida é utilizada para decifrar os dados cifrados recebidos
  - Desta forma é feita cifragem/decifragem apenas da chave secreta (máx 256 bits)

Criptografia Assimétrica Serviços – Assinatura Digital

- Assinatura Digital
  - Serviço semelhante a uma assinatura manual. Neste caso a assinatura é gerada por uma entidade e outras podem verificar e atestar sua veracidade
  - Considerando que a chave privada (PR) é de conhecimento apenas do seu proprietário, a assinatura fica garantida pois a mesma é é criada com a chave privada (PR) e então é verificada com a chave pública(PU)
  - Como os dados a serem assinados pode ser de qualquer tamanho uma função Hash pode ser utilizada a fim de obter um sumário de tamanho fixo dos dados a serem assinados
  - Processo de criação
    - O assinante criar uma hash dos dados e obtém uma saída de tamanho fixo
    - O assinante então cifra o hash com sua chave privada (PR)
  - Processo de verificação
    - O destinatário produz um hash dos dados recebido
    - A assinatura recebida é decifrada utilizando a chave pública (PU) do assinante e compara com o hash produzido. Se iguais a assinatura é válida.

Criptografia Assimétrica Serviços - Integridade

- Integridade de dados
  - A assinatura digital garante:
    - A autenticidade da origem dos dados (informação sobre quem produziu a assinatura)
    - A integridade dos dados, indicando que os mesmos não foram alterados de nenhuma forma
  - A assinatura digital não garante a confidencialidade dos dados
  - As premissas acima são verdadeiras se:
    - Somente o assinante possui a chave privada
    - Não é possível obter, na prática, a chave privada a partir da chave pública

Criptografia Assimétrica Serviços – Key Exchange

- Troca de Chaves (Key Exchange)
  - Permite o uso de criptografia assimétrica a fim de permitir a troca de chaves secretas entre duas entidades
  - O protocolo utiliza as chaves públicas (PU) e privadas (PR) a fim de que permitir o compartilhamento de uma chave simétrica secreta (K)
  - O processo pode ser feito de suas formas:
    - Transferência de Chaves (Key Transfer) – Neste caso uma entidade produz a chave simétrica (K) e a envia para a outra entidade. A criptografia assimétrica pode ser utilizada a fim de garantir a confidencialidade
    - Concordância de Chaves (Key Agreement) – Ambas as entidades colaboram na geração da chave simétrica
    - Exemplo: DIFFIE-HELLMAN

Infra-estrutura - Conceito

- Consiste de recursos disponíveis e prontos para ser utilizado por diferentes consumidores através de uma interface previamente definida
  - Exemplos: Infra-estrutura Elétrica e Infra-estrutura de Redes
- A infra-estrutura é como uma caixa preta que oferece serviços
- A infra-estrutura de segurança deve ser acessível por todas as aplicações e objetos que necessitam de serviços de segurança
- A infra-estrutura evita o uso de soluções incompletas, que não se intercomunicam e além disso permite o gerenciamento consistente da segurança entre aplicações tanto dentro de uma organização, quanto entre organizações.
- Considere a falta da infra-estrutura de energia elétrica. Seria possível?
- A PKI pode formar a base da infra-estrutura de segurança, porém não é a infra-estrutura de segurança em seu todo
- Em um PKI os serviços são implementados utilizando conceitos de técnicas da criptografia de chave pública

PKI – Public-Key Infraestructure
Infra-estrutura de chave pública

- A PKI é a base uma infra-estrutura de segurança onde os serviços são implementados e executados através de conceitos e técnicas disponíveis na criptografia de chave pública
- Entre os serviços e componentes necessários em uma PKI temos:
  - Autoridade Certificadora (Certification Authority)
  - Repositórios de Certificados (Certificate repository)
  - Revogação de Certificado (Certificate Revocation)
  - Recuperação e Backup de Chaves (Key backup and recovery)
  - Atualização de Chaves (Automatic key update)
  - Gerenciamento de Histórico de Chaves (Key history management)
  - Certificação Entre Domínios (Cross-certification)
  - Suporte para Não-Repudio
  - Tempo Identificado (Time stamping)
  - Software Cliente

Certificados

- Na criptografia de chave pública a chave pública pode e necessita ser distribuída entre as partes que se comunicam.
- A distribuição desta chave pública sem critério algum poderia comprometer os serviços de segurança
  - A chave pública deve ser protegida de alguma forma sem no entento comprometer a escalabilidade do sistema de criptografia baseada em chaves públicas
  - Além disso certos atributos precisam ser adicionados a uma chave pública
  - É necessário garantir a integridade dos dados da chave pública, bem como de outras informações associadas, a fim de garantir que não foram indevidamente modificadas
  - Somente a garantia da integridade de dados não é suficiente para garantir que o proprietário da chave pública é quem afirma ser.
  - É necessário um mecanismo que associa a chave pública a seu proprietário de uma maneira confiável
- Para os fins descritos acima são utilizados os certificados.

Certificados – Mundo Real

- Documento que:
  - Contem uma afirmação
  - É passível de verificação pelo seu emissor
  - É fornecido com cuidados
  - Exemplos do mundo real:
    - Certificado de Diploma; Nascimento; Morte; Casamento; Certificado de Compra; etc.
  - Além disso o certificado pode conter
    - Número identificador
    - Período de Validade
    - Uma assinatura
    - Um selo

Certificados Digitais

- Um certificado pode ser definido como um estrutura de dados cujo objetivo é associar o nome de uma entidade, bem como outras de suas características a sua chave pública
- Existem diferentes tipos de certificados
  - Certificados de chave pública X.509
  - Certificados Simples de Infra-Estrutura de Chave Pública – SPKI (Simple Public Key Infrastructure) certificates
  - Certificados PGP (Pretty Good Privacy)
  - Certificados de Atributos
- Além disso um mesmo tipo de certificado pode apresentar:
  - Diferentes versões
  - Extensões Opcionais, permitindo o uso em aplicações específicas
    - Secure Electronic Transaction (SET) certificates

Certificados PGP

- PGP (Pretty Good Privacy) é um meio criado essencialmente para cifrar e assinar digitalmente e-mails e arquivos
- A última versão, conhecida como OpenPGP, foi publicada como um padrão IETF através da RFC 4880
- Existem diferenças significativas entre os Certificados PGP e o X.509 versão 3
- Além disso os modelos de confiança são completamente diferentes
- Desta forma existe uma separação entre a comunidade que utiliza PGP e que utiliza X.509
- A versão mais atual do OpenPGP suporta tanto os certificados PGP, como os certificados X.509, porém ainda existem incompatibilidades entre os protocolos OpenPGP e S/MIME (Secure / Multipurpose Internet Mail Extensions) que utilizam o X.509
- Em geral o PGP está voltado para o usuário final e o certificado X.509 voltado para corporações.

Certification Authority (CA)

- Uma autoridade certificadora (Certification Authority) é a responsável pela emissão de certificados de chave pública
- Os certificados são assinados com a chave privada da CA emissora
- Desta forma os mesmos estão protegidos do ponto de vista da integridade, podendo então ser disseminados de acordo com a necessidade
- Existem modelos públicos e privados para a disseminação de certificados
- Para maiores informações no Brasil visite o site do ITI

Certificado X.509

- O certificado X.509 possui a seguinte estrutura:
  - A versão 3 (version 3) é a última versão disponível atualmente

Version 1
Version
Serial Number
Signature
Issuer
Validity
Subject
Subject's Public-Key Information
Issuer Unique ID
Digital Signature

Version 2
Version
Serial Number
Signature
Issuer
Validity
Subject
Subject's Public-Key Information
Issuer Unique ID
Subject Unique ID
Digital Signature

Version 3
Version
Serial Number
Signature
Issuer
Validity
Subject
Subject's Public-Key Information
Issuer Unique ID
Subject Unique ID
Extensions
Digital Signature

Certificado X.509 - Estrutura

- Version
  - Indica a versão do certificado por ser 1, 2 ou 3
- Serial Number
  - Número inteiro fornecido pela entidade certificadora (CA) relativo ao certificado
- Signature
  - Algoritmo utilizado para calcular a assinatura digital e parâmetros relacionados
- Issuer
  - Nome da CA
  - Utiliza o padrão de nome definido na recomendação X.500, conhecido como DN (Distinguished Name)
  - O objetivo é que o nome seja único
  - Um DN é constituído da uma concatenação de RDN (Relative Distinguished Names) a partir do topo (ou raiz) de um diretório
  - Contém os campos C (Contry); O (Organization); OU (Organization Unit); L(Locale); S (State); CN (Common Name)
- Validity
  - Indica o período do tempo em que o certificado é valido (Valid From; Valid To)

Certificado X.509 - Estrutura

- Subject
  - Nome do proprietário do Certificado
  - Utiliza o padrão de nome definido na recomendação X.500, conhecido como DN (Distinguished Name) a fim de que o nome seja único
  - Um DN é constituído da uma concatenação de RDN (Relative Distinguished Names) a partir do topo (ou raiz) de um diretório
  - Contém os campos C (Contry); O (Organization); OU (Organization Unit); L(Locale); S (State); CN (Common Name)
- Subject's Public-Key Information
  - A chave pública do proprietário do Certificado
  - Inclui também o nome do algoritmo utilizado e outros parâmetros necessários
- Issuer Unique Id e Subjet Unique Id
  - Um identificador opcional do emissor do certificado. Presente somente nas versões 2 e 3
  - Raramente utilizado na prática e seu uso não é recomendado pela RFC 3280
- Subjet Unique Id
  - Um identificador opcional proprietário do certificado. Presente somente nas versões 2 e 3

Certificado X.509 – Estrutura Extensões (Extensions)

- Consiste de um conjunto de um ou mais campos opcionais, presentes apenas na versão 3 a fim de proporcionar flexibilidade no formato do certificado
- Cada Extensão possui:
  - Um identificador (identifier);
  - um flag (critically flag) que caso seja verdadeiro indica que esta extensão é crítica e precisa ser entendida e processada, caso contrário o certificado não pode ser utilizado. Caso o campo seja falso a extensão pode ser processada mas caso ocorra algum erro a mesma será ignorada
  - O valor da extensão (extension value)
  - Certificate Policies
    - Indica uma sequência de uma ou mais políticas, representadas por seus OIDS (Object Identifiers) e qualificadores associados
    - Se marcado como crítico a aplicação deve aderir a pelo menos uma das políticas indicadas
    - Apesar da RFC3280 recomendar que estas extensões não sejam usadas a fim de promover a interoperabilidade a mesma define pois possíveis qualificadores:
      - Certification Practice Statement (CPS) – um URI (Uniform Resource Identifier) da política
      - User Notice Qualifier – Uma nota de referência sobre a política

Certificado X.509 – Estrutura Extensões (Extensions)

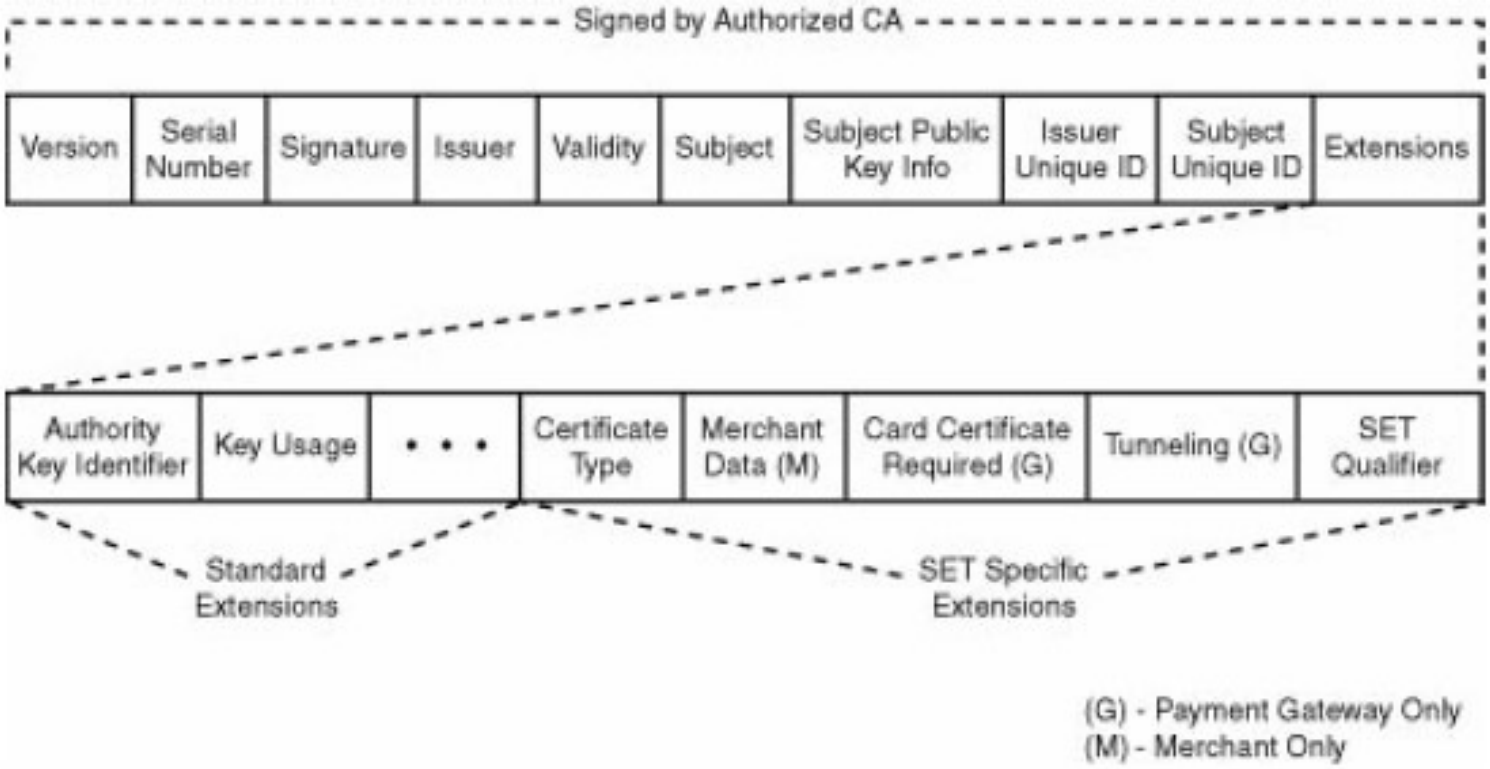
- Certificate Revocation List (CRL) Distribution Point
  - Indica a localização de uma CRL (Certicate Revocation List) reside
  - Uma CRL é uma estrutura de dados, digitalmente assinada, que contém uma lista dos certificados revogados.
  - A lista pode ser assinada pelo emissor do certificado (CA) ou por outra entidade
- Subject Key Identifier
  - Um identificador único associado com a chave pública contida no certificado
  - Seu objetivo é distinguir entre múltiplas chaves associadas ao mesmo proprietário do certificado
  - Este campo é obrigatório para certificados de uma CA
- Authority Key Identifier
  - Um identificador único da chave que deve ser utilizada para verificar a assinatura digital associada ao certificado
  - Permite distinguir entre múltiplas chaves associadas ao mesmo emissor do certificado
- Basic Constraints
  - Indica se o certificado é de uma entidade certificadora (CA)
  - Normalmente este campo não está presente em certificados de um usuário final

Certificado X.509 – Estrutura Extensões (Extensions)

- Key Usage
  - Uma string de bits utilizada para identificar ou restringir as funções ou serviços que são suportados pelo certificado
  - Pode indicar suporte para:
    - assinatura digital;
    - não repúdio;
    - cifragem de chaves;
    - cifragem de dados;
    - compartilhamento de chaves (key agreement);
    - assinatura de certificado;
    - assinatura de CRL (Certificate Revocation List);
    - apenas cifragem;
    - apenas decifragem
  - Normalmente contém uma combinação dos serviços acima
- Existem outras extensões padrão possíveis definidas na RFC 3280
- Além das extensões padrão é possível ainda extensões específicas para uma aplicação

Certificado X.509 – Estrutura Extensões (Extensions) Específicas

- Além das extensões padrão previstas na RFC 3280, é possível ainda que o certificado possua extensões específicas para uma aplicação
- Um exemplo é o Secure Electronic Transaction (SET)
  - Este padrão define os requisitos necessário para o pagamento com cartão de crédito de transações comerciais em redes de comunicação como a Internet, por exemplo



Gerenciamento de Chaves e Certificados

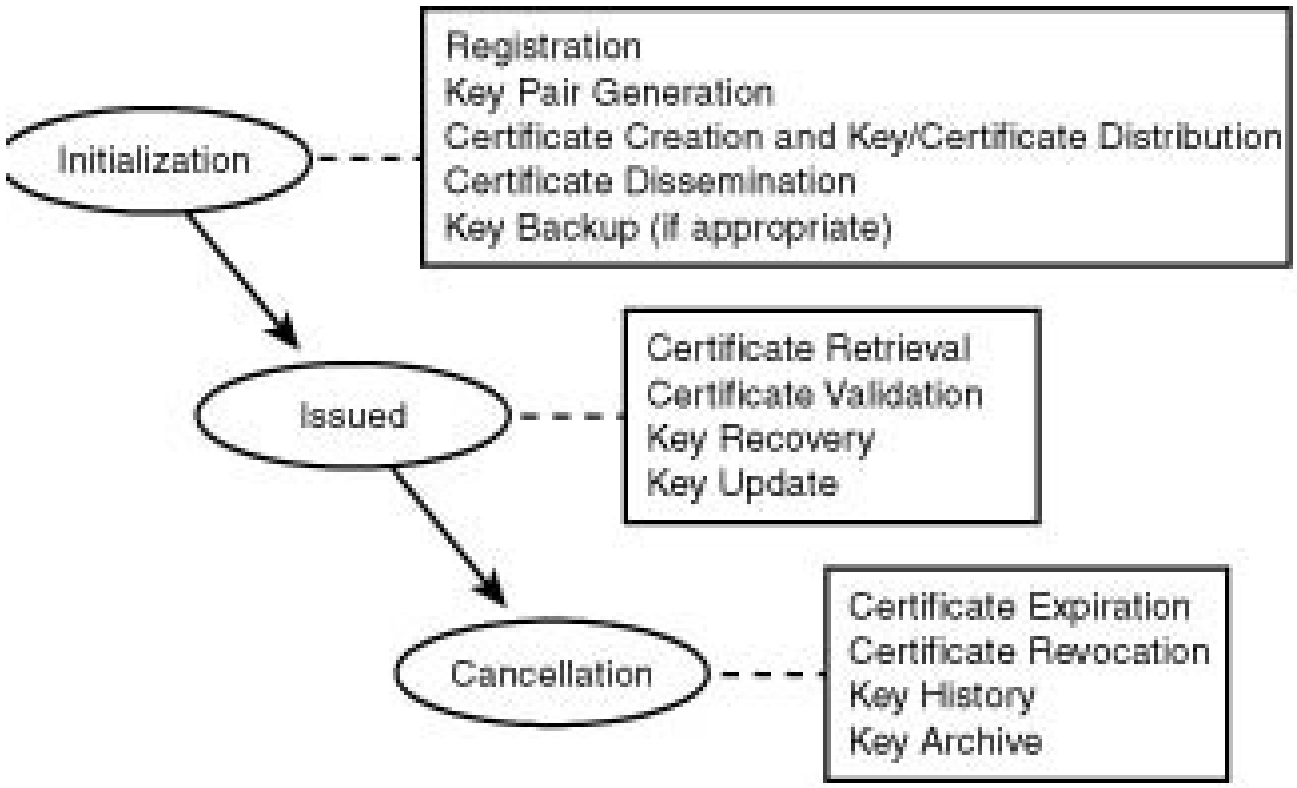
- O ciclo de vida de uma chave e o certificado possui várias fases
  - Inicialização
  - Utilização
  - Cancelamento
- Nem todas as fases acima são necessárias e podem eventualmente não ocorrer
- A infra-estrutura de chave pública deverá oferecer os serviços conforme a necessidade

Gerenciamento de Chaves e Certificados - Serviços

- Serviços existentes em cada fase
  - Inicialização
    - Registro da Entidade Final (End-Entity Registration)
    - Geração do Par de Chaves (Key Pair Generation)
    - Criação e Distribuição do Certificado (Certificate Creation and
    - Key/Certificate Distribution
    - Disseminação do Certificado (Certificate Dissemination)
    - Backup da Chave (Key Backup)
  - Utilização
    - Recuperação do Certificado (Certificate Retrieval)
    - Validação de Certificado (Certificate Validation)
    - Recuperação de Chaves (Key Recovery)
    - Atualização de Chaves (Key Update)
  - Cancelamento
    - Finalização de Certificado (Certificate Expiration)
    - Revogação do Certificado (Certificate Revocation)
    - Gerenciamento do Histórico de chaves (Key History)
    - Arquivamento de Chaves (Key Archive)

Gerenciamento de Chaves e Certificados

- Fases de uma chave e seu certificado



Fase de Inicialização

- Uma entidade precisa ser inicializada na PKI
- Para isto existe o processo de inicialização
- O processo é composto das seguinte fases
  - Registro da Entidade Final (End-Entity Registration)
  - Geração do Par de Chaves (Key Pair Generation)
  - Criação e Distribuição do Certificado (Certificate Creation andKey/Certificate Distribution
  - Disseminação do Certificado (Certificate Dissemination)
  - Backup da Chave (Key Backup)

Registration Authority

- Para entrar em uma PKI é necessário o registro.
- Este serviço pode ser efetuado por uma CA (Certifcation Authority) porém normalmente este serviço é feito por um componente (ou entidade) específica, chamada Registration Authority (RA)
- Considerando que o número de entidades finais (end entities) está em constante crescimento e que normalmente estão geograficamente dispersas a noção de um local centralizado para registro pode ser um problema
- O objetivo da RA é retirar a carga do processo de registro da CA a fim de aumentar a escalabilidade e reduzir custos
- Uma RA pode ser ainda subdividida, de acordo com a legislação vigente, em múltipas RAs, conhecidas como Local Registration Authorities (LRA)
- Funções de uma RA
  - Estabelecer e confirmar a identidade de uma entidade que deseja se registrar em uma PKI
  - Iniciar o processo de certificação junto a uma CA
  - Produzir chaves em nome do usuário
  - Executar certos processos como iniciar um processo de cancelamento de um certificado
- Uma RA nunca pode emitir certificados ou CRL (Certificate Revocation List)
- O custo de um certificado digital, obtido publicamente, pode variar, para maiores informações veja o exemplo de uma autoridade de registro

Fase de Inicialização

- O processo de inicialização pode ocorrer de várias formas uma delas é mostrada a seguir